

EAG:SEF
F.#2008R01454

M10-1413

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- - - - - X

UNITED STATES OF AMERICA

SUBMITTED UNDER SEAL

- against -

AFFIDAVIT IN SUPPORT
OF AN ARREST WARRANT

USMAN MALIK,
SAIF ALI CHAUDHRY,
 also known as "Faif
 Chaudhry,"
MUHAMMAD ASIF,
 also known as "Sumera
 Tassawer,"
and
MUHAMMAD ALI,

(18 U.S.C. §§ 1349,
and 3551 et seq.)

Defendants.

- - - - - X

EASTERN DISTRICT OF NEW YORK, SS:

OLIVER GRANT, being duly sworn, deposes and states that he is a Special Agent with the United States Secret Service, duly appointed according to law and acting as such.

Upon information and belief, in or about and between June 2007 and May 2010, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants USMAN MALIK, SAIF ALI CHAUDHRY, also known as "Faif Chaudhry," MUHAMMAD ASIF, also known as "Sumera Tassawer," and MUHAMMAD ALI, together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud

and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted, by means of wire communication in interstate commerce, writings, signs, signals and sounds, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

The source of my information and the grounds for my belief are the following:

BACKGROUND

1. I have been a Special Agent with the United States Secret Service since 1999. As such, I have been involved in numerous investigations and prosecutions of electronic crimes and access device fraud. In the course of those and other investigations, I have conducted physical surveillance, executed search warrants, debriefed cooperating defendants and confidential informants, reviewed computer records and secured other relevant information using other investigative techniques.

2. I am familiar with the facts and circumstances of this matter from: (a) my personal participation in this investigation; (b) reports made available to me by other law enforcement officials; and (c) records made available by T-Mobile.

3. Except as explicitly set forth below, I have not distinguished herein between facts of which I have personal knowledge and facts as to which I have hearsay knowledge.

4. Because this affidavit is being submitted for the limited purpose of seeking authorization to arrest the defendants USMAN MALIK, SAIF ALI CHAUDHRY, also known as "Faif Chaudhry," and MUHAMMAD ALI, I have not set forth each and every fact determined during the course of this investigation, but simply those facts which I believe are necessary to establish probable cause for the requested arrest warrant.

PROBABLE CAUSE

A. **Background**

5. Cellular telephone service providers are typically charged "transit" fees for calls by their customers that are routed over the networks of other telephone service providers. Transit fees often include "termination" fees, which are charged by the company that provides telephone service to the call recipient. Termination fees are particularly high in countries such as Liechtenstein, Nauru and Sierre Leone ("high termination-fee countries").

6. Since approximately June 2007, agents of the United States Secret Service have been investigating the use of T-Mobile cellular telephone numbers that have been obtained by fraudulent means in an effort to produce a high volume of

telephone calls from the United States and several foreign countries to telephone numbers in high termination-fee countries, as part of an apparent scheme to share in the resulting termination fees.

7. The scheme involves the use of several techniques to obtain fraudulent access to T-Mobile cellular accounts. For example, one technique involves adding new cellular telephone numbers to the existing accounts of valid T-Mobile customers, without the knowledge or consent of those customers. Another technique involves activating new cellular accounts using personal information obtained from existing or past T-Mobile customers, or from other individuals and business entities, without the knowledge or consent of those individuals or entities.

8. Subscriber Identity Module ("SIM") cards are portable computer chips used to power certain types of cellular telephones. SIM cards can be moved among cellular telephone handsets. Each SIM card is assigned a unique identifying number, known as an International Mobile Subscriber Identity ("IMSI") number.

9. Each handset within which a SIM card is used has its own unique identifying number, known as an International Mobile Equipment Identity ("IMEI") number. A single handset may be used with multiple SIM cards. When a cellular telephone

handset using a SIM card places or receives a call, the cellular provider records both the SIM card and the specific handset used.

10. Each SIM card is associated with a particular telephone number. As a result, a user can make calls from a single telephone number even while using multiple different handsets, and without notifying the cellular service provider in advance, simply by transferring the SIM card to a new handset. Similarly, because a handset can be used with multiple SIM cards, a user can use a single handset to make calls from multiple phone numbers.

B. The Criminal Scheme

11. The defendant USMAN MALIK has been a T-Mobile customer since at least June 4, 2005. MALIK is the registered user of a SIM card with the IMSI number 310260912853154 (the "MALIK SIM card").

12. The defendant SAIF ALI CHAUDHRY, also known as "Faif Chaudhry," was a T-Mobile customer on or about and between May 1, 2007 and July 13, 2010.

13. The defendant MUHAMMAD ASIF, also known as "Sumera Tassawer," was a T-Mobile customer on or about and between November 8, 2007 and January 16, 2009, when the account was closed by T-Mobile for nonpayment. The ASIF account was registered with T-Mobile under the name MUHAMMAD ASIF at a residential address in Brooklyn, New York. A T-Mobile account

in the name of "Sumera Tassawer" was opened on or about July 30, 2009 and remains open. The Tassawer account is registered with T-Mobile at the same street address in Brooklyn, New York as that of the ASIF account. On November 5, 2010, ASIF was photographed by a T-Mobile surveillance camera at a T-Mobile store in Brooklyn, New York making a payment on the account registered in Tassawer's name. On November 27, 2010, the undersigned agent spoke to ASIF. ASIF's voice appeared to match that of an individual who identified himself as Tassawer in calls to T-Mobile concerning the account registered in Tassawer's name.

14. The defendant MUHAMMAD ALI has worked at Cellfonz R Us, a cellular telephone store with locations in Brooklyn, Queens and Long Island, New York that sells T-Mobile products and services. Since June 2007, at least 48 customers of Cellfonz R Us have had T-Mobile accounts activated in their names, without their knowledge or consent, and those accounts were subsequently used to place high volumes of calls to high termination-fee countries.

15. On numerous occasions since June 2007, cellular telephone handsets used to make calls with SIM cards assigned to the personal T-Mobile cellular telephone accounts of defendants MALIK, CHAUDHRY and ASIF have also been used to place a high volume of calls to telephone numbers in high termination-fee

countries using SIM cards associated with fraudulently obtained T-Mobile cellular accounts.

16. For example, since June 2007 at least 16 cellular telephone handsets used to place and receive calls using the MALIK SIM card were also used to place a high volume of calls to telephone numbers in high termination-fee countries using approximately 361 SIM cards associated with fraudulently obtained T-Mobile accounts.

a. For example, on February 4, 2008, the cellular handset with the IMEI number 359039011218430 was delivered by United Parcel Service to a residential address registered with T-Mobile as belonging to MALIK.¹ The handset was used to place calls using the MALIK SIM card between February 4, 2008 and May 15, 2008. The same handset was also used between April 10, 2008 and April 27, 2008 to place calls to telephone numbers in India, Pakistan, Kuwait, Saudi Arabia, East Timor, Sao Tome and the Philippines using three SIM cards associated with fraudulently obtained T-Mobile accounts. According to cell-site information obtained from T-Mobile, one of those SIM cards placed calls almost exclusively from the vicinity of a T-Mobile cell

¹ On April 9, 2010, the undersigned agent observed MALIK emerge from that residence and walk in the direction of a nearby shopping mall. On November 26, 2010, the undersigned agent again observed MALIK emerge from that residence, enter a car and drive away.

site located adjacent to a residence that was registered with T-Mobile as belonging to CHAUDHRY.²

b. Similarly, the cellular handset with the IMEI number 010737005874190 was used on February 28, 2009 to place calls using the MALIK SIM card. Between May 31, 2007 and March 17, 2009, the same handset was used to place a high volume of calls to telephone numbers in Liechtenstein, India, Pakistan, Sao Tome, the Czech Republic, Sierra Leone, Austria, East Timor, Zimbabwe, and Saudi Arabia, using 34 SIM cards associated with fraudulently obtained T-Mobile accounts.

c. Similarly, on March 5, 2009, the cellular handset with the unique IMEI number 011539007766930 was used with the MALIK SIM card as well as with a SIM card registered to a fraudulent T-Mobile account. Between March 3, 2009 and June 2, 2009, the same handset was used to make a high volume of calls to telephone numbers in high termination-fee countries using five SIM cards associated with fraudulently obtained T-Mobile accounts.

17. Since June 2007, at least 16 cellular handsets used to place and receive calls using SIM cards registered to CHAUDHRY were also used to place a high volume of calls to telephone numbers in high termination-fee countries using

² On November 17, 2010, agents of the investigative agency observed CHAUDHRY emerge from that residence, enter a car, and drive away.

approximately 129 SIM cards associated with fraudulently obtained T-Mobile accounts.

a. For example, between October 4, 2008 and October 20, 2008, the cellular handset with the unique IMEI number 359304010294070 was used to place and receive numerous calls using a SIM card registered to CHAUDHRY. Between September 29, 2008, and April 2, 2009, the same handset was used to place a high volume of calls to Sierra Leone using three SIM cards associated with fraudulently obtained T-Mobile accounts.

b. Similarly, between February 22, 2009 and March 21, 2009, the cellular handset with the unique IMEI number 358265013118520 was used to place and receive calls using SIM cards registered to CHAUDHRY. Between March 19, 2009 and June 26, 2009, the same handset was used to place a high volume of calls to Sierra Leone using SIM cards associated with fraudulently obtained T-Mobile accounts.

18. Since June 2007, at least 5 cellular handsets used to place and receive calls using a SIM card registered in the name "Sumera Tassawer" were also used to place a high volume of calls to telephone numbers in high termination-fee countries using approximately 33 SIM cards associated with fraudulently obtained T-Mobile accounts. One of those handsets was also used with SIM cards registered to ASIF; two of those handsets were also used with SIM cards registered to CHAUDHRY.

a. For example, between September 4, 2009 and November 1, 2009, the cellular handset with the unique IMEI number 011714001970470 was used to place and receive numerous calls using a SIM card registered to Tassawer. Between September 10, 2009 and September 24, 2009, the same handset was used to place a high volume of calls to telephone numbers in high termination-fee countries using SIM cards associated with fraudulently obtained T-Mobile accounts.

b. Similarly, between August 4, 2009 and September 29, 2009, the cellular handset with the unique IMEI number 359304010294070 was used to place and receive calls using a SIM card registered to Tassawer. Between September 29, 2008 and April 2, 2009, the same handset was used to place a high volume of calls to telephone numbers in high termination-fee countries using SIM cards associated with fraudulently obtained T-Mobile accounts.

19. On numerous occasions, the defendants MALIK, CHAUDHRY, ASIF and ALI have called T-Mobile and used the personal information of existing or past T-Mobile customers, or of other individuals and business entities, without the knowledge or consent of those individuals or entities, to activate T-Mobile cellular accounts that were subsequently used to place high volumes of calls to telephone numbers in high termination-fee countries. When calling T-Mobile to activate wireless accounts

using fraudulent information, the defendants impersonated authorized T-Mobile dealers by using seven digit "dealer codes" assigned to those dealers.

a. For example, since December 2007, approximately 93 T-Mobile accounts were fraudulently activated using a dealer code, 0097896, which is assigned to an authorized T-Mobile dealer located in Brooklyn. Those accounts were later used to place a high volume of calls to telephone numbers in high termination-fee countries. Twelve of the fraudulently activated accounts were linked to SIM cards that were, in turn, used to place calls with cellular telephone handsets that were also used with the MALIK SIM card. Eight of the fraudulently activated accounts were linked to SIM cards that were, in turn, used to place calls with cellular telephone handsets that were also used with SIM cards registered to CHAUDHRY.

b. On December 10, 2007, a T-Mobile customer, John Doe, added an extra line of service to his existing T-Mobile account through Cellfonz R Us, in Brooklyn. Thereafter, on December 31, 2007, another T-Mobile account was activated in John Doe's name, but without John Doe's knowledge or consent, using the same dealer code, 0097896, referenced above. Minutes after the fraudulent account was activated, an individual who identified himself as "Mike A" and claimed to be an authorized T-Mobile dealer called a T-Mobile customer care center located in

Meridian, Idaho to change the billing address on the fraudulent John Doe account. The call was consensually recorded by T-Mobile as part of its ordinary business practices. The caller's voice appears to match that of an individual who identified himself as the defendant ALI in other calls to T-Mobile concerning the valid accounts of Cellfonz R Us customers. On January 2, 2008, the fraudulent John Doe account was disconnected after T-Mobile security officials discovered that it had been used to place a high volume of calls from New York to Sao Tome. The handset used to place the calls to Sao Tome was also used between August 10, 2007 and February 4, 2008 to place and receive calls using the MALIK SIM card.

c. On October 13, 2008 and March 14, 2009, an individual called T-Mobile using fraudulent information to activate accounts that were subsequently used to place a high volume of calls to telephone numbers in high termination-fee countries. The call was consensually recorded by T-Mobile as part of its ordinary business practices. The caller's voice appears to match that of an individual who identified himself as the defendant CHAUDHRY in other calls to T-Mobile concerning CHAUDHRY's personal account.

d. On September 9, 2009 an individual called T-Mobile using fraudulent information to activate an account in the name of a corporate entity, Holiday Inn Express. The caller's

voice appears to match that of ASIF in ASIF's conversation with the undersigned agent on November 27, 2010, as well as that of the individual who identified himself as Tassawer in calls to T-Mobile concerning the account registered in Tassawer's name. Between September 9, 2009 and September 12, 2009, the SIM card associated with the fraudulently obtained Holiday Inn Express account was used to place a high volume of calls to telephone numbers in high termination-fee countries using the cellular handset with the unique IMEI number 011886002407740. On September 9, 2009, that same handset was also used with a SIM card registered to CHAUDHRY. Between September 10, 2009 and September 15, 2009, the SIM card associated with the fraudulently obtained Holiday Inn Express account was also used to place a high volume of calls to telephone numbers in high termination-fee countries using the cellular handset with the IMEI number 011714001970470. As noted above, this same handset was used on or about and between September 4, 2009 and November 1, 2009, to place and receive calls using a SIM card registered to Tassawer. According to cell-site information obtained from T-Mobile, international calls made using the fraudulently obtained Holiday Inn Express account during the period on or about and between September 9, 2009 and September 13, 2009, were placed from various locations in New York, central Pennsylvania, western Maryland, West Virginia, Virginia and North Carolina. SIM cards

registered to CHAUDHRY and Tassawer were in those same locations on or about those same dates.

e. On at least seven separate occasions between July 2008 and March 2009, an individual called T-Mobile using fraudulent information to activate accounts that were subsequently used to place a high volume of calls to telephone numbers in high termination-fee countries. The caller's voice appears to match that of an individual who identified himself as the defendant MALIK in other calls to T-Mobile concerning MALIK's personal account.


20. The personal T-Mobile SIM cards of defendants MALIK and CHAUDHRY have also been used to place numerous calls to foreign companies that advertise the opportunity to profit from calls to "premium-rate" telephone numbers.

a. For example, since May 2007, more than 134 calls have been placed from a T-Mobile account registered to MALIK to a telephone number listed as a contact number on the website of Maxtis Telecom, a company based in the Czech Republic that advertises the opportunity to share in the revenue from calls to "premium-rate" telephone numbers.

b. There have been at least two calls between a T-Mobile account registered to CHAUDHRY and a contact number for Maxtis Telecom.

c. Similarly, there have been at least 42 telephone calls and text messages exchanged between a T-Mobile account registered to MALIK and a telephone number listed as a contact number on the website of Premium TLC, a company based in Belize that advertises the opportunity to share in the revenue from calls to "premium-rate" telephone numbers, including numbers in several high termination-fee countries.

WHEREFORE, I respectfully request that the Court issue arrest warrants for the defendants USMAN MALIK, SAIF ALI CHAUDHRY, also known as "Faif Chaudhry," MUHAMMAD ASIF, also known as "Sumera Tassawer," and MUHAMMAD ALI, so that they may be dealt with according to law, and that this Affidavit and the arrest warrants be filed under seal to prevent the flight of the defendants.



OLIVER GRANT
Special Agent
United States Secret Service

Sworn to before me this
51st day of November, 2010



UNITED
EASTERN

S/Levy

DGE
K